European Economic and Social Committee

Record of processing activity
Part 1

Name of the data processing	Videosurveillance
Created on	19/09/2018
Last update	
Reference number	008
Year	2018
1. Controller:	European Economic and Social Committee
2.a) Service responsible	SECU
2b) contact details	secu@eesc.europa.eu
3. Joint controller	Not applicable
4. DPO: contact details	data.protection@eesc.europa.eu
5. Processor(s) (where applicable)	Not applicable
6. Purpose(s) of the data processing	

	The Committees use their video-surveillance system for the sole purposes of security and access control. The video-surveillance system helps control access to EESC-CoR buildings and helps ensure the security of buildings, the safety of staff and visitors, as well as property and information located or stored on the premises. It complements other physical security systems such as access control systems and physical intrusion control systems. It forms part of the measures to support EESC-CoR broader security policies and helps prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises and protected rooms, IT infrastructure, or operational information. In addition, video-surveillance helps prevent, detect and investigate theft of equipment or assets owned by the Committees, visitors or staff, and threats to the safety of visitors or personnel working at the office (e.g. fire, physical assault). The system is not used for any other purpose. For example, it is not used to monitor the work of employees or to monitor attendance. The Committees do not use covert surveillance.
7. Description of the categories of persons whose data are processed	EESC and CoR staff - EESC and CoR members - Visitors - External Security company - Any other person likely to enter the Committees' buildings - Demonstrators passing in front of the Committees' buildings
8. Description of data categories processed	Video images digitally recorded. Due to the location of their buildings and in order to fulfil their security needs, Committees video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership.
9. Time limit for retaining the data	Footage is retained for a maximum of 30 days. Thereafter, all images are automatically erased by the system which overwrites on data older than 30 days. In case of security incidents, due to administrative procedures, it might take up to a month for judicial and/or police authorities to request recordings necessary for investigating security incidents. Some images may be stored longer if they are retained as part of an investigation or as evidence of a security incident. Their retention is rigorously documented and the need for retention is periodically reviewed. Images of demonstrators are retained for 48 hours only, due to the nature of data collected (special categories of data might be collected, such as political opinions, religious or philosophical beliefs, trade union membership). This period is necessary in order to identify whether security incidents have occurred (for example, damage to buildings).

10. Recipients of the data	In-house security staff and outsourced security-guards. Recorded video is accessible to in-house security staff only. Live video is also accessible to security guards on duty. These security guards work for an external security company. Local police may be given access if needed to investigate or prosecute criminal offences. In the course of investigating crimes or offenses or in order to prosecute, images may be transmitted to the Belgian Federal or Local Police. Such requests for disclosure must be reasoned, submitted in writing to the Security Service and must comply with the formal and content requirements imposed by the national legislation in force. Whenever possible and independently of the obligations imposed at the national level, the Committees will request a judicial warrant, a written request signed by a sufficiently high ranked police officer or a similar formal request. The request should also specify, as accurately as possible, why the video surveillance sequence is required as well the exact place, date and time of the sequence requested. If the police or another national organisation of a Member State makes a request for access under an official procedure, it must first obtain a waiver of immunity if the sequence in question concerns a member of an Institution of the Union. Under exceptional circumstances, access may also be given to: - the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF, - the Commission's Investigation and Disciplinary Office ("IDOC") in the framework of a disciplinary investigation, under the rules set forth in Annex IX of the Staff Regulations of Officials of the European Communities, or - those carrying out a formal internal investigation or disciplinary procedure within the Institution, provided that it can be reasonably expected that the transfers may help investigation or prosecution of a sufficiently serious disciplinary offence or a criminal offence.
11. Transfers of personal data to a third country or an international organisation	Not applicable
12. General description of security measures, where possible	

	Restricted access: recorded video is accessible to the Committees in-house security staff only. Live video is accessible to security guards on duty. Premises hosting the servers storing the footage are protected by physical security measures. Network firewalls protect the perimeter of the IT infrastructure. The main computer systems holding the data are security hardened. Administrative measures include the obligation of all outsourced personnel having access to the system (including those maintaining the equipment and the systems) to be individually security cleared. All staff (external and internal) signed non-disclosure and confidentiality agreements. Access rights to users are granted only to those persons who need them in order to carry out their jobs. Only the system administrator specifically appointed by the controller for this purpose is able to grant, alter or annul access rights of any persons. The log-in and use of the system is traceable to a particular user.
13. Privacy statement	Video-surveillance
Part 2 Compliance check and risk screening	
1.a) Legal basis and reason for processing	☑ (a) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body ☐ (b necessary for compliance with a legal obligation to which the controller is subject (see point 1b) below) ☐ (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ☐ (d) the data subject has given consent to the processing of his or her personal data for one or more specific purposes ☐ (e) necessary in order to protect the vital interests of the data subject or of another natural person [Tick (at least) one of the boxes]
1b) Legal basis	
2. Are the purposes specified, explicit and legitimate?	Yes, the use of our video-surveillance system is necessary for the management and functioning of the Committees (for security and access control purpose)
3. Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	The system is not used for any other purpose.
4. Do you really need all the data items you plan to collect?	

5. How do you ensure that the information you process is accurate?	
6. How do you rectify inaccurate information?	
7. Are they limited according to the maxim "as long as necessary, as short as possible"?	Yes. There are no cameras elsewhere either in the building or outside of it. Areas under heightened expectations of privacy such as individual offices, leisure areas, toilet facilities and others are not monitored. Cameras do not focus on the faces of individuals and do not seek to identify individuals unless there is an imminent threat to public safety or violent behaviour. Monitoring outside EESC-CoR buildings on Belgium territory is limited to an absolute minimum.
8. If you need to store certain information for longer, can you split the storage periods?	Yes. Footage is retained for a maximum of 30 days. Images of demonstrators are retained from 48 hours only, due to the nature of the data collected.
9 How do you inform data subjects?	Information to the public about the video-surveillance is provided in an effective and comprehensive manner: - on-the-spot notices to alert the public to the fact that monitoring takes place and provide them with essential information about the processing - a public version of the video-surveillance policy is available on intranet and internet - print-outs of video-surveillance policy are also available at building reception desks and from security unit (secu@eesc.europa.eu) upon request Notices are posted at all entrances to the Committee's buildings, including the entry to the parking lot.
10. Access and other rights of persons whose data are processed	Any request for access, rectification, blocking and/or erasing of personal data should be directed to the security service (secu@eesc.europa.eu). Whenever possible, the security service responds to an enquiry in substance within 15 calendar days.
11. Does this process involve any of the following?	☐ (a) data relating to health, (suspected) criminal offences or other special categories of personal data ☐ (b) evaluation, automated decision-making or profiling ☑ (c) monitoring data subjects ☐ (d) new technologies that may be considered intrusive

Part 3
Linked documentation

1. Links to threshold assessment and DPIA (where applicable)	No hyperlink inserted
2. Where are your information security measures documented?	No hyperlink inserted
3. Links to other documentation	No hyperlink inserted
4. Other relevant documents	